



DOI User Guide

Remote Access to
DOI Time and Attendance

This IT service provided by



Table of Contents

Table of Contents.....	2
Introducing Remote Access to DOI Time and Attendance.....	3
Accessing DOI Time and Attendance from Outside the DOI Network (No VPN Required)	3
Additional Information Regarding the New Website	7
Frequently Asked Questions	8

Introducing Remote Access to DOI Time and Attendance

DOI's IT Transformation is making it easier for U.S. Department of the Interior (DOI) employees to submit their time and attendance on a regular basis.

Most DOI employees use the DOI Time and Attendance application daily. However, a DOI network connection has always been required to access it. This makes it hard for DOI's diverse workforce with employees who may travel often or be in remote locations, sometimes far from their home offices. These employees need to be able to input their time and attendance at any time from any location.

To address this need, DOI's IT Transformation has enabled remote access to DOI Time and Attendance for DOI employees through a new externally accessible website.

Currently, this new website does not support the Bureau of Reclamation's time and attendance system, E-Tas. Remote access to DOI Time and Attendance is an additional way for employees to enter their time and attendance and does not replace all current methods.

Accessing DOI Time and Attendance from Outside the DOI Network (No VPN Required)

Step 1: Establish Web Browser Security

To begin, employees need to establish the proper security settings for their web browsers. The website for accessing DOI Time and Attendance requires a Transport Layer Security (TLS) encryption. The device being used to access the website must have a TLS-enabled web browser. Directions to correctly configure different web browsers to enable TLS are provided below.

Using Internet Explorer:

1. Open Windows Internet Explorer
2. Click on the Tools tab (See Figure 1)
3. Select Internet Options (See Figure 1)
4. Click the Advanced tab (See Figure 2)
5. Scroll down to find “Use TLS 1.0” (See Figure 2)
6. Check the “Use TLS 1.0” box (See Figure 2)
7. Click Apply (See Figure 2)
8. Close and exit

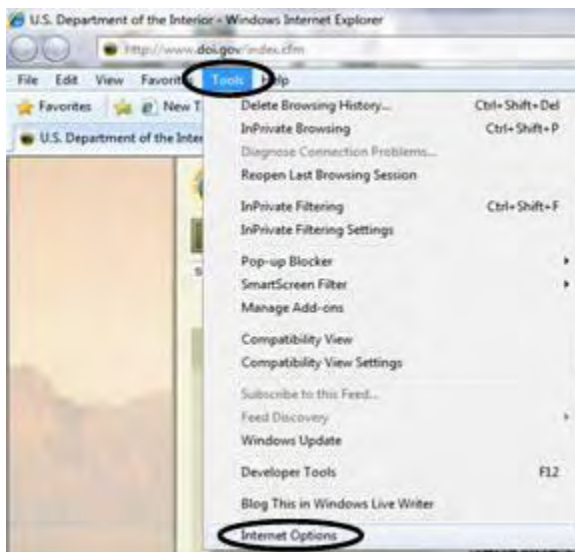


Figure 1



Figure 2

Using Firefox:

1. Open Mozilla Firefox
2. Open the Firefox toolbar
3. Make the following menu selections: Options -> Options
4. Select the Encryption Tab
5. Ensure “Use TLS 1.0” option is selected
6. Close the options window

Using Google Chrome:

1. Open Google Chrome
2. Click the wrench icon on the right hand side
3. Choose Options
4. Select Under the Hood tab (See Figure 3)
5. Click Change proxy settings (See Figure 3)
6. Select the Advanced tab (See Figure 3)
7. Scroll down and check “Use TLS 1.0” (See Figure 3)
8. Click Apply (See Figure 3)
9. Close and restart all open browsers

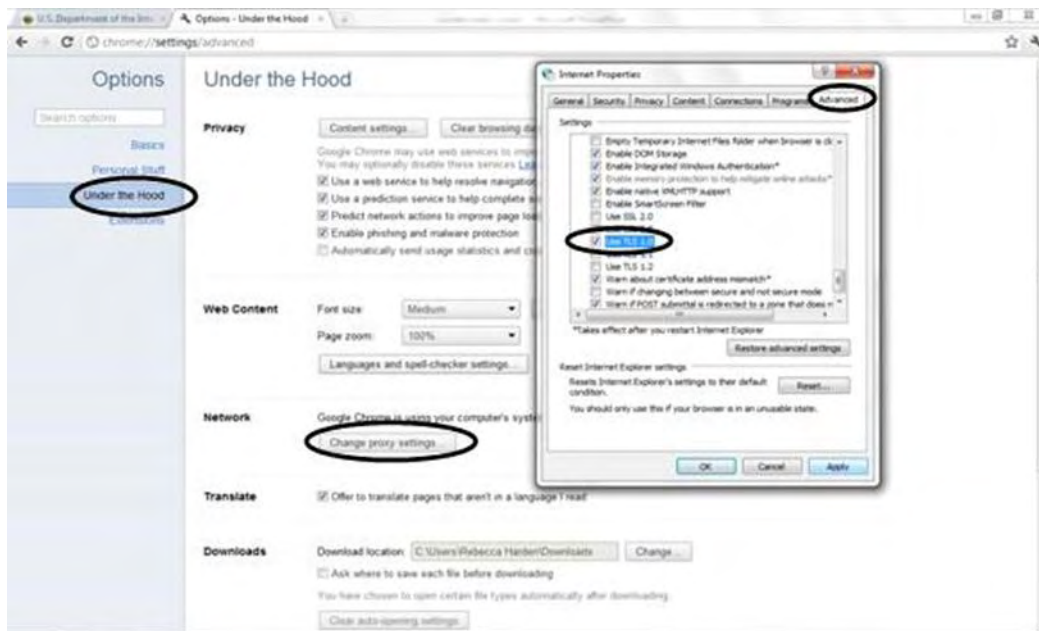


Figure 3

Using Safari:

The Safari browser enables TLS use by default. No further action is needed.

Step 2: Connect to DOI Time and Attendance

Once an employee's web browser is configured for TLS encryption, the next step is to visit the public website for accessing the DOI Time and Attendance application.

1. Go to <https://apps.doi.gov>
2. Enter username. This is what you use to login to your computer – your Active Directory username. You also need to add the @fill-in-bureau.gov. See FAQs for more details.
3. Enter password and click "Connect"

U.S. Department of the Interior

DOI Application Access

DOI Access Card

Step 1: Insert your DOI Access card into the card reader
Step 2: Click "Connect"

Connect

Username and Password

Step 1: Enter your username and password below
Step 2: Click "Connect"

username

password

Connect

If your T&A is sponsored by a different bureau than your username please click this link: [All Bureau T&A Links](#)

Contact Support: Please contact your local helpdesk if you require additional assistance. [Help](#)

WARNING TO USERS OF THIS SYSTEM This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, recorded, copied and used for authorized purposes at any time. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

4. After a successful connection, you will see the following screen. Click on the appropriate DOI Time and Attendance link which will vary based upon your bureau or office.

U.S. Department of the Interior

[Home](#) [Preferences](#) [Logout](#)

Enterprise Remote Access Services Secure Access Portal, daniel.stoll

WARNING TO USERS OF THIS SYSTEM This computer system, including all related equipment, networks, and network devices (including Internet access), is provided by the Department of the Interior (DOI) in accordance with the agency policy for official use and limited personal use. All agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded, copied and used for authorized purposes at any time. All information, including personal information, placed or sent over this system may be monitored, recorded, copied and used for authorized purposes at any time. Therefore, there should be no expectation of privacy with respect to use of this system. By logging into this agency computer system, you acknowledge and consent to the monitoring of this system. Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution. [Collapse](#)

Web Bookmarks

- [BIA T&A](#)
Time and Attendance for Bureau of Indian Affairs.
- [BLM T&A](#)
Time and Attendance for Bureau of Land Management.
- [BOEM T&A](#)
Time and Attendance for Bureau of Ocean Energy Management.
- [BSEE T&A](#)
Time and Attendance for Bureau of Safety and Environmental Enforcement.
- [FWS T&A](#)
Time and Attendance for Fish and Wildlife Employees.



You will now be connected to time and attendance. Proceed as usual.

Additional Information Regarding the New Website

THE “BROWSING” BAR: As employees use the new website to access DOI Time and Attendance or other internal web applications, they will see a bar at the top right corner of their screen. This bar provides:

- A link to www.doi.gov
- A link to the website’s home page for easy navigation within the secure environment
- A session counter which counts down the maximum length of the session
- Help and exit icons



The  button will move the bar to the left hand side of the browser window, and the  button will collapse the browser bar to a minimum view. These options are available in the event that the browser bar is in the way of normal page viewing.

When employees are finished entering their time and have logged out of DOI Time and Attendance, they need to make sure to click the Exit icon to log off the website and close the browser.

Frequently Asked Questions

Q: *What exactly is the new website?*

A: The new website securely allows employees with a web browser to access certain DOI applications on both Government Furnished Equipment (GFE) and now on Personally Owned Equipment (POE). Initially, the website will only allow employees to access DOI Time and Attendance and the DOI intranet, oneINTERIOR. Additional services will be added in the future. The website is also accessible to employees in the event of a man-made or natural state of emergency.

Q: *Do I need to be authorized to use the VPN in order to access the new website?*

A: No. In order to access the VPN (Virtual Private Network) an employee must have suitable GFE equipment and be specifically authorized to do so. The website is designed to allow all DOI staff with a DOI email address to access DOI resources without having to log into the VPN. The website is also accessible on Personally Owned Equipment (POE).

Q: *I have received the error message “Invalid username or password.” What should I do?*

A: Make sure to use the correct Active Directory username and password. Your username is what you use to login to your computer. The website also requires that employees use the “@fill-in-bureau” suffix format. The following is a list of bureau suffixes/domains:

BIA = @indianaffairs.gov

FWS = @fws.gov

BLM = @blm.gov

MMS = @mms.gov (for ONNR, BOEM, BSEE)

BOR = @usbr.gov

NBC = @nbc.gov

NPS = @nps.gov

OSM = @osmre.gov

OHA = @oha.doi.gov

OST = @ost.doi.gov

OHTA = @ohta.doi.net

SOL = @sol.doi.gov

OS = @ios.doi.gov

USGS = @usgs.gov

Q: *I have received the error message “Account Disabled or Locked.” What should I do?*

A: Employees should contact their bureau’s help desk and let them know that their account has been locked out.

Q: *Can I use my DOI Smart Card to log into the website?*

A: Yes, but it is not necessary to use a DOI Smart Card to access the website. The website allows employees to use their DOI Smart Card for authentication on GFE. Insert the smart card into the card reader, open the browser, go to <https://apps.doi.gov>, and click connect under the DOI Access Card box. Employees will be prompted to enter their PIN number and select the proper certificate. If employees receive a “Wrong Certificate” message, they should close their browser and try again by selecting the other certificate. It’s a good idea to write down the correct certificate as the browser will always present them in the same order.

Q: I received a message after 25 minutes stating that my session will be logged out unless I click “continue.” Why am I receiving this message?

A: OMB directs that all remote access services must drop connections after 30 minutes of inactivity. If employees connect to the website and remain inactive, they will be reminded 5 minutes prior to the system automatically dropping the connection that their session will be discontinued. To avoid having to re-enter their username and password again, employees should click “continue” on the 5-minute warning message. This ensures that employees continue to maintain a secure connection to the DOI network.

Q: I closed the browser window or tab and have lost the browser bar and no longer have access. How do I get it back in to the system?

A: During your secure session, employees should always see the browser bar at the top of the screen. If they open a new tab or browser window, it will not have access through the secure portal. It is important to keep the current window with the browser bar open. If the connection is lost, employees should go back to <https://apps.doi.gov>, enter their username, password and click connect. They may be notified that they have a “Session in progress.” If so, click “Continue this session.” The old session will be terminated and the employee will be logged back in.

Q: I have multiple windows open with the Access Browser Bar. How did this happen and which one should I use?

A: This is a result of the DOI web page opening up a pop up window. The browser bar indicates that it is a secure connection. Employees should not be concerned, as this is normal. They will be able to interact with the pop up or the original window. If you like, you can simply close the pop up window.

Q: I do not have a laptop, but I have a tablet device. Can I still use this service?

A: Yes, the website was specifically designed to allow any TLS web-enabled device to access DOI resources. This includes GFE and POE such as iOS devices (iPhone, iPad, iPod touch), Android devices, Windows Mobile, Windows OS (XP, Vista, 7) OSX (Panther – Lion).

Q: I am detailed to the Department or another bureau/agency. I use the account where I am detailed for logon purposes, but my home bureau/office still manages my payroll in DOI Time and Attendance. Unfortunately when I logon to the website using the detailed account, I do not see the correct Time and Attendance link. What can I do?

A: Your situation applies to only a very few individuals. In order to help you, we have provided a different link so you can see all the instances of DOI Time and Attendance for DOI organizations. Please navigate to <https://apps.doi.gov/qtall> and select the appropriate link for your purposes.

Q: It doesn't work. What should I do?

A: The good news is that DOI Time and Attendance access via the website is an alternative method of inputting time and attendance information. Employees can always access DOI Time and Attendance by using GFE either on the internal network or by using the VPN.

Although DOI does not support troubleshooting for personal devices, there are a few steps employees can take to fix their particular issue themselves including:

- 1) Verify they have Internet access. Try to navigate to a well-known site like Google. Does it appear?
- 2) Verify compliance with the "Establish Web Browser Security" section earlier in this document. Does the employee's device have a TLS enabled web browser? If so, are they actually using TLS 1.0?
- 3) Verify they entered the website correctly. It is <https://apps.doi.gov> Do they see the correct webpage?
- 4) Test to see if the system works on another POE device. Again, DOI will not provide support for personal devices, but if it works on the second device then at least the employee knows the challenge is isolated to the first device.
- 5) The employee may have challenges with their account. They should verify their ability to log into the DOI network using GFE on either the internal network or VPN.
- 6) Contact someone else to see if it works for them. If it does not work for them, then perhaps something is wrong with the system. If DOI is experiencing Internet outages, then the system may be offline. Wait until the service is restored. If the service doesn't appear to be affected, it is suggested that employees wait an hour and then retry. If multiple parties with multiple devices are not able to access the system, then a call to the Help Desk would be in order to ensure the system is operating normally.

Q: How do I *add an employee, change a SSN, or view a SSN as a Timekeeper or Administrator on the website?*

A: Timekeepers and Administrators are not allowed to add employees, change SSNs, or view SSNs while using the website. In order to access these functions, log onto DOI Time and Attendance through your normal means of connection. The website protects sensitive personally identifiable information (PII), including employees' SSN.

Q. *The drop down menu isn't working correctly to select "Self" or "Alternate" to certify timesheets*
What should I do?

A: During testing, issues selecting "Self" or "Alternate" on the drop down menu existed, particular on Android devices. For staff who certify timesheets and are confronted with this behavior, use one of the following options to solve the issue:

- Use another device
- Certify timesheets using government furnished equipment over the Virtual Private Network (VPN)
- Use your normal means of certifying

Q: *Do I need to use a smartcard with my personally owned device to access the website?*

A: No, you do not need to use a smartcard with your personally owned device to access services on the website. If your personal device is capable of using a smartcard, and if you desire to use a smartcard, you may use it. At this time there is no expectation that government funds will be expended to support personally owned equipment or the associated hardware/software. You may also use any smart card capable government furnished equipment to access the website, should you so desire.